Security and Privacy for IoT Data Through Trust Management System by using Cluster Based Management

Meena Sachdeva[1], Davinder Kumar[2]

JIMS Engineering Management Technical Campus, Gr., Noida, India[1]

Micron Technology, Hyderabad, Telangana, India[2]

Corresponding author: Meena Sachdeva, Email: meena.sachdeva255@gmail.com

Internet of Things (IoT) networks has been evolving phenomenally over the past two decades. Although the devices generally hold relatively low memory, resource and processing capability, the challenge with its trend is that nodes generate a vast volume of data. That is where cloud technology kicks off to offer storage space. An extensive network functioning with cloud assistance might be vulnerable due to its centralized nature and robustness. Besides, the devices may be exposed to malicious activities due to weak access control policies. However, cloud technology provides a platform on which such a security system can execute. Within the framework of these criteria, a centralized, secure architecture fails to consider the mobile and edge devices. This raises many questions about the trust in third-party cloud intermediaries that cause security and privacy leakages. This paper presents trust management system mechanism as an excellent component providing security solution in the network which not just lessens device's energy consumption enhances the network lifetime, as well offers a proficient trust model to guarantee the network is treated as reliable, free from any sort of malicious attackers in the IoT system. This describes cluster priority based IoT system with their advantages.

Keywords: Trust Management, IoT, Cluster Priority Based Trust Management

2023. In Deepak Bhatia & Himanshu Arora (eds.), *SCRS Proceedings of International Conference of Undergraduate Students 2023*, 61–74. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.56155/978-81-955020-4-2-7

1. Introduction

The power of individuals to control and better their lives has increased thanks to the Internet of Things (IoT), which has made it possible for an increasing number of intelligent gadgets and smart sensors to be connected. However, security issues are starting to surface with IoT, and one of the challenges is the coexistence of solutions from various vendors, standards, protocols, and community groups. In the present study, we address the issue of identifying IoT devices by analysing a set of packets from its high-level network traffic, i.e., network-flow data, and extracting unique flow-based attributes to produce a fingerprint for each item. We utilise supervised machine learning methods for the identification task. The suggested approach has the ability to automatically identify connected devices as well as specific instances of white-listed device types. We also offer a security system model architecture that enables the implementation of rules for limiting connections from IoT devices in accordance with their assigned privileges. Trust Management System of Internet of Things: Managing the trust in IoT devices that are heterogeneous is a very challenging task compared to other kinds of network domains like WSN, MANET, P2P, Grid, Delay Tolerant, etc. There are different approaches adopted for trust management to propose a dynamic protocol to achieve its objectives [1], [2]. Mainly, we have to implement distributed trust management for IoT looking at the pressing and serious issues it faces to maintain security, privacy, access control, device identification, and management in real-world applications [3]. The trust management system for optimal performance classifies the design into five different components, which are explained below their contributions involving specific attributes and properties in Fig. 1.1

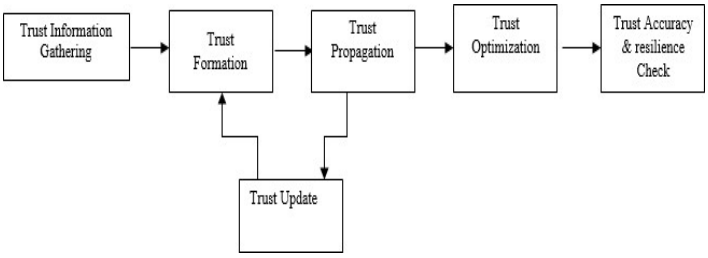

Fig . 1.1. Trust Management System Model

Trust information gathering: Initial step of this model, which focuses on the trust or and trustee device properties, their service requirements, and network properties. The information is collected through knowledge, experience, and reputation means Trust Formation: Essential step for trust computation decides the number of trust properties that are going to be considered to evaluate the trust. Generally, the classification of trust property is realized as single or multiple trusts. Also, after designing the trust evaluation model, this component will analyze the effect of trust results on network performance measured parameters. Trust Propagation: Dissemination of the trust information is augmented in the IoT environment through direct and indirect communications. Further, indirect communication is inferred from historical transaction information of the recommender nodes which provides feedback on the node's behavior.

2. Trust Accuracy and Resilience Check

Trust management solution is evaluated against the objectives like trust convergence, trust accuracy, and resilience. Trust Optimization: Elucidate the importance of less energy consumption and a high trust level efficient solution to establish trust between unknown physical entities in the IoT environment. Moreover, this solution can be extended to handle scalability, the large scale of device participation in applications. Trust Update: Update trust value of devices based on trust evaluation results from the recent trust information. It's the event driven specific which means trust values are

calculated and updated once the event is triggered. There are certain prevalent approaches followed to design trust management systems such as centralized (objective approach) and distributed (subjective approach). Looking at security requirements at IoT, the most appropriate would be distributed approach not only it has dynamic adaptability in response to a dynamically changing environment, but also support scalability to accommodate the vast number of IoT devices.

3. Distributed Approach

In this scheme, each entity contributes towards the process of information exchange when they interact with each other without any central entity control. Hence, the advantage of using a distributed approach without a centralized entity is that no single point of failure during operation time can affect the trust management execution processes [4], [5]. This type of approach has been certainly realized the reduced efficacy on memory management, computation cost, and convergence time. Centralized (objective approach): Instead of each entity, in this scheme, the central entity takes the charge of all trust computation and decision making. To calculate trust about a device, the provider will request the centralized unit which will do the trust evaluation needful and acknowledge the device about the decision [6]. The efficacy of this approach is trust computation is global and done by the physical cloud, outside of the device layer so there is less chance of tampering of trust data but a high risk of the single point of failure is foreseen during devices interactions with the centralized unit.[7-9]

4. Attacks on Trust

Trust management aims to manage the trust between entities where one entity finds the trustworthiness of another entity through an automated mechanism before utilizing/providing services or resources [10], [11]. It's a challenging task to maintain trust between heterogeneous devices. Despite having an efficient trust management solution, the IoT system is still vulnerable and compromised by malicious nodes. The effects of adversaries are so detrimental to the network performance, that hamper the cooperation among distributed nodes, and extremely arduous to find these nodes to keep them out of network operations. Adversaries can perform against trust management systems through these different categories of attacks Fig.1.2.

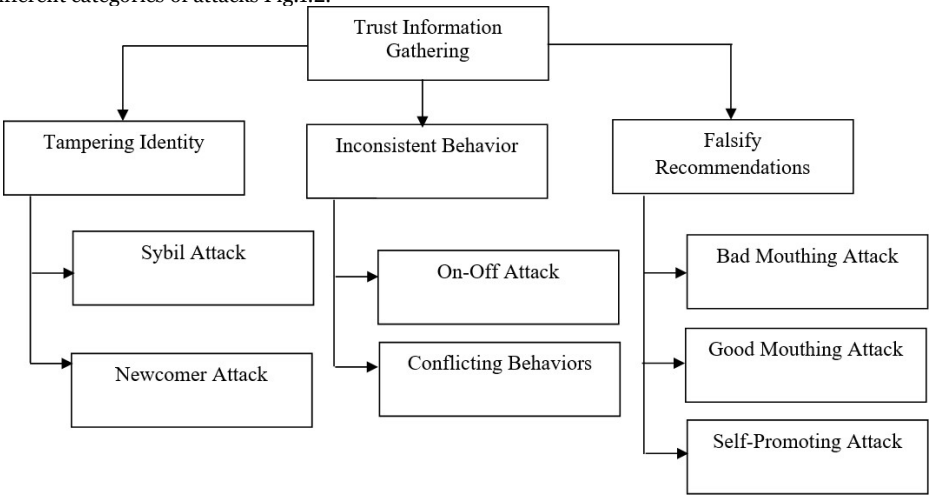

Fig.1.2. Trust Management Attacks

Tampering Identity Management: Here nodes will tamper with their device identity and issue fake identity to the network. Sybil Attack: It will be seen in the information gathering phase of the trust management system. By breaching the authentication mechanism, the malicious node will create fake ids for nodes to disrupt the network performance.

Newcomer Attack: This attack is also present in the information gathering phase of the trust management system. The malicious node will erase its bad history and will come up with a new identity to join the network.
Inconsistent Behavior: Node will behave differently during operation time with other nodes.

On-Off Attack: This attack is observed in trust formation and dissemination phases and provides good and bad services alternatively, the behavior is unpredictable and difficult to detect.

Conflicting Behavior Attack: Malicious node provides different types of feedback score to other nodes; it's not the same feedback score to be shared.

5. IoT Architecture

The different layers of architecture in IoT show that the reliability of the network. Three, four, and five-layered architectures are available in IoT Fig. 1.3. Each layer in an IoT provides more security. The architecture provides more concentration on the factors which are affected by the system. After the development, it is increasing rapidly and its technologies are adopted by the users. There are many processes done through the internet of things like processing, passing data, security, confidentiality, transaction used by sensing the devices. Through the technique that the system can be used anywhere at any time the communications are also possible with IoT [12], [13].

Prevention of attack is done by the layers of the architecture and they provide the solution to the attacks. IoT is mainly achieving communication between different domains and nodes. Several communications are done through IoT, so security will be needed. The division of each layer provides each type of security. The architecture describes the following features as follows:

Develop a layered architecture and each layer shows the different types of attack in IoT. Provide a proper security mechanism in each attack. Elaborate the layer for more security like four-layered to five-layered. The development of technologies needs more security. At first, three layered architecture was proposed. After the development of more technologies in the internet of things, the requirements and functionalities have not fulfilled the layers. So for more security purposes four-layered and five-layered architecture introduced. Increasing technologies and the need for security architecture are increased rapidly in an IoT environment. The functions of architecture are to the position of an object, the presence of a new object, detection of a place in which the objects are placed.[14-15]

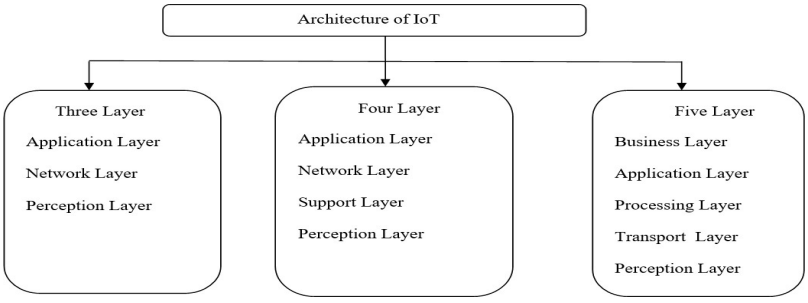

Fig.1.3. IoT Architecture

6. Challenges in IoT

A huge number of devices are connected to the IoT internet world, so there are many open issues and challenges present. The first challenge is the standardization to provide a uniform approach to all the technologies used in IoT platforms [16].
Active and Passive Attacks: These attacks can disrupt the communication of the network and retrieve sensitive data. Threats in an IoT are from both internal and external entities of the system. Unavailability of resources at that time makes the delay of service delivery in a network. Outdated hardware and software of devices are not upgraded and very much prone to attacks. No prevention technologies are available in IoT to protect the users' data privacy. Data are not protected with the use of conventional cryptographic algorithms and key management. Multiple devices are responsible for packet transmitting over the network; need an efficient traffic management technique. Traffic analysis helps to set the special rules for data transmission and receive to avoid any loss or collision. Data mining is another issue. It allows the sensitive data to be visible to other users. Authentication and identity management. Identity management needs to offer a capable solution to prevent the devices from indulging in duplicating their identities. Another challenge is trust management and integration policies. Trust management does not have a subjective agreement. Providing access control to the appropriate resource is a major issue in this network. No single networking protocol to secure the system from malicious attacks. The new invention of the protocol is not an easy one and the network protocol wants to completely fulfill the user's requirements. The selection of a correct topology is also another issue. Interaction between the systems, there should a solution to allow seamless Interoperability operations. Because many devices are connected to the common environment with different properties and formats which generates the data overhead. Scalability, due to the changing of an environment the system wants a capacity to grow up their features. The main issue is that the people cannot make any changes in a system when they change the environmental conditions.

Preservation: The system can be easily hacked by others. Infrastructure is another challenge of trust in the internet of things. Due to the huge number of devices, the one system that wants to find and interact with the other system is more difficult.

7. Advantages of IoT

Transmission: IoT supports the data transmission between devices and can remain associated with lesser failures and more remarkable quality [17].
Automation Control: Without human intervention, the devices can sense and transmit with one another, sending the vast amount for processing and analysis to cloud servers.
Time Saving: Time saved due to IoT technologies is a very great effort, which attracts the customers to have this experience
Better Quality of Life: All this innovation has increased comfort, accommodation, and better administration, consequently improving the quality of life.
Monitor: The main advantages of IoT sensors are their sensing capabilities and capture sensitive/critical data in a harsh environment. Through these erroneous data, different analytic functions will take as input and generate valuable decision-making outputs.
Better User Experience: The analyzed data or reports are reaching out to the users through web applications or mob apps. Also, gathers the user experiences through the reports and improves further.
Lower Operation Costs: This IoT infrastructure is not the fixed number of hardware and software to achieve the application objectives. IoT level varies from Level 1 to Level 2 based application requirement [18]. The customer has the flexibility to decide what kind of level will fulfill the application productivity.

8. System and Threat Model

In this part, we present a design for a security identification, authentication, and enforcement paradigm. Our suggested generic solution uses a switch or gateway to link IoT devices to the network using a wireless or wired IP-network, which may be utilised in both the residential and commercial sectors.[19-20] IoT devices connected to a network infrastructure are recognized by the model, allowing them to join and set their network rights. IoT devices already connected to the network will also be routinely checked against a baseline in order to confirm the accuracy of the identification and discover any malicious or misbehaving devices. Threat Restricting each related department's rights in accordance with predetermined standards. [21]These pre-established standards categorise devices into different privilege zones according to the importance of their communication and data, so defining where they should be put.[22] Contrasting the current device's actions with a baseline established through regular communication between the two to help in the detection of rogue (mistakenly classed as approved) or compromised devices and to restrict their access to network resources and privileges for further monitoring.

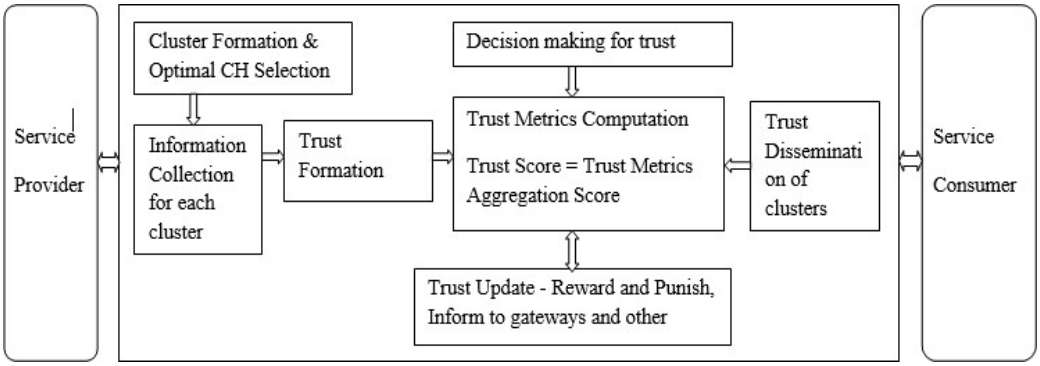

Fig.1.4. System and Threat Model

Cluster Priority Based Trust Management Protocol The proposed trust based model concentrates on fundamental issues of IoT and prominently, will address the issue of authentication, access control, data integrity, and privacy through a trustworthy platform. Further, nodes of the network are formulated into different clusters based on the initial setup phase of LEACH cluster formation model. Each cluster is composed of CH (cluster head) and CMs (cluster members), where the CH of each cluster is selected for its resource richness and is expected to have longer battery life, more storage capacity with the ability to perform on intra-cluster and inter-cluster appeals [23-27]. Now in the edge computing layer, the important job of edge nodes is to monitor and collect information from CHs in the perception layer. Edge nodes with current CHs together will find the optimal CH for each cluster through trust model defined metrics, which involve the trust calculation. Moreover, making trust evaluation accuracy high, Identifying impactful trust parameters for the trust model, and selecting dynamic mathematical formulas for trust aggregation, then the computation is very crucial for designing and developing the holistic trust management protocol.

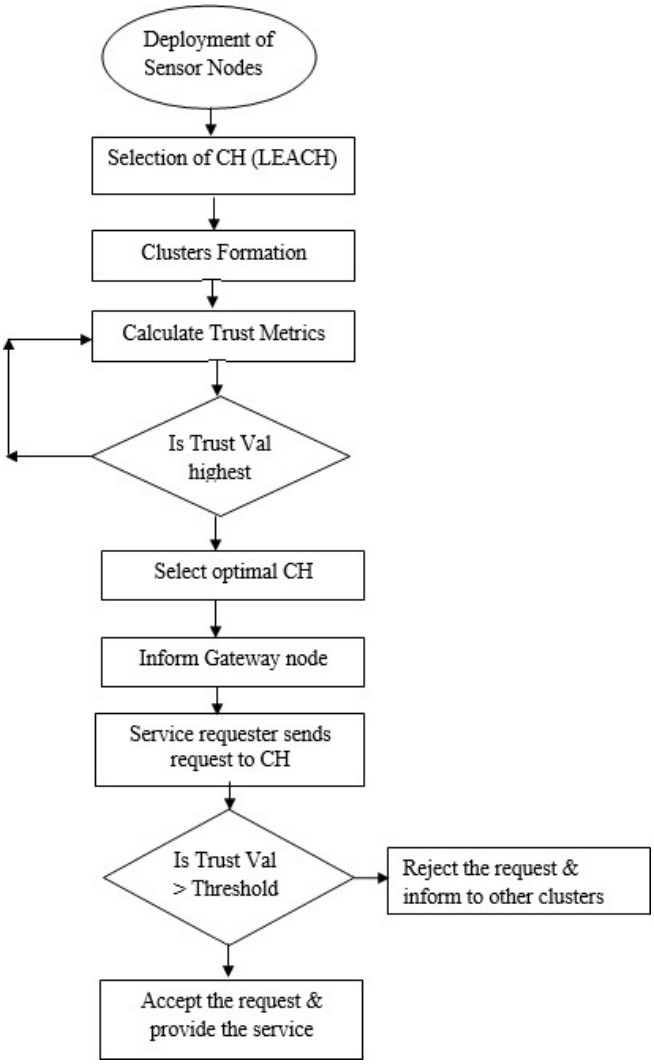

Fig. 1.5. Flowchart of LEACH protocol with Trust Metrics

Fig. 1.5 depicts an overview of trust management architecture comprising main physical entities and between them, intermediate layer trust management steps are displayed. Initially, cluster formation and optimal CH selection process started before interactions with the service provider or requester.[28] The trust formation step defines multi-dimensional properties to be considered for trust computation to have fast trust convergence and high trust accuracy [29]. Decision making step outlines the best suitable trust model based device properties and available trust information. Finally, the trust dissemination step includes the direct and indirect response of devices during interactions so that communication among the devices inside and outside the cluster will be continued. Based on the trust

value result, CH will provide feedback on the requester node of other clusters through the edge node.[30-34] The complete flow of the trust management approach is displayed in Fig. 1.4. Many IoT application devices are low in energy and low computation power that makes these devices vulnerable to attacks, therefore our trust management solution provides a secure solution to device-to-device communication. The detailed algorithm suggests how CH and edge nodes coordinate each other to handle physical entities interactions without intruding on the malicious nodes [35]–[37]. Also, to improve the network lifetime and efficient energy consumption, the complete trust evaluation process is done only by the cluster head for every cluster, whereas in earlier research works service provider was handling this activity and consumes more energy for trust evaluation process execution and update of trust value. The trust model dynamic weighted sum (DWS) approach was adopted for our protocol for assessing the trust scores, which defines trust metrics for computation. It includes all trust properties which are obtained during the trust formation phase. The uniqueness of this model shows important aspects of trust management functions, which consider direct observations, indirect observations, edge node information trust for selecting optimal CH and then, direct observations, residual energy, required energy after nodes with assigned security groups, community groups, provider common elite buddies, and finally, additional checkpoints of provider and consumer nodes.

Trust Metrics is characterized for optimal CH selection from the below equation
$TV^{(CH)} = W_1DIT + W_2IIT + W_3NC + W_4EIT$

$TV(^{CH})$: Trust estimation for cluster head DIT: Direct interaction trust of the node
IIT: Indirect interaction trust from other nodes

NC: Neighbor nodes count
EIT: Edge nodes information trust

Where, W1, W2, W3, and W4are weight constants and floating between 0 to 1decided based on the intricacy of IoT applications and environmental uncertainty.
Despite energy consumption in local processing inside the cluster for selecting CH, still it provides multifold benefits to the network. It reduces considerably overall communication overhead inside at sensing layer and outside to gateway node at edge computing layer, so it reduces the energy consumption of devices for unnecessary and malicious interactions.[38-42] For a network, improved network lifetime decides how good the trust management solution stands for the pressing issues that nodes are facing in the IoT paradigm. As both reduced communication overhead cost and reduced energy consumption established our solution as a holistic one could address the core issue of device interaction security.[43-44]

Algorithm:
Information: IoT Network of devices placed randomly having fixed range of communication [45]
Step-1: IoT devices in the network are forming different clusters utilizing clustering model LEACH and node density inside each cluster will remain the same.

Step-2: Identify the optimal cluster head, then our distributed methodology inside that group, where residual, required energy, direct trust, and reputation values are considered,

- $PL(CH,J) = RE_I + REQDE_I + TVal_{Node}$
- CH: Cluster head, I: Service Provider, and J: Service requester
- PL(CH,J) = Performance Level of Custer Head w.r.to service requester J
- RE_I=Residual Energy of service provider I
- $REQDE_I$= Required Energy of service provider I
- $TVal_{Node}$ = Direct trust estimation of CH to J
- PL(Threshold) = Performance Threshold Level
- Integrated PL(CH) = PL(CH,J) + Rep(CH,J)
- Reputation, $Rep(CH,J) = \sum (W_k D_{kj})$,

Where k nodes outside its cluster, i.e. from gateway nodes PL (Threshold) is determined by the edge node depending on the application requirement and device properties. The node having the highest PL(CH) for intra cluster or Integrated PL(CH)for inter cluster and above threshold level PL(Threshold) then the node is considered for resource allocation at this moment, otherwise, node requests will be turned down.

Step-3: CH will maintain key-value pair information for every node inside its cluster, key will be the identity of the member and value will keep CM's properties like communication protocols, services, trust value.

Step-4: Based on the service request, the provider's CH will initiate trust assessment and trust evaluation of the requester's CH and its appealed node.

Step-5: Calculated the integrated trust value compared with the threshold value, it will be decided if the resource will be allocated to the requester node or not based on the result.

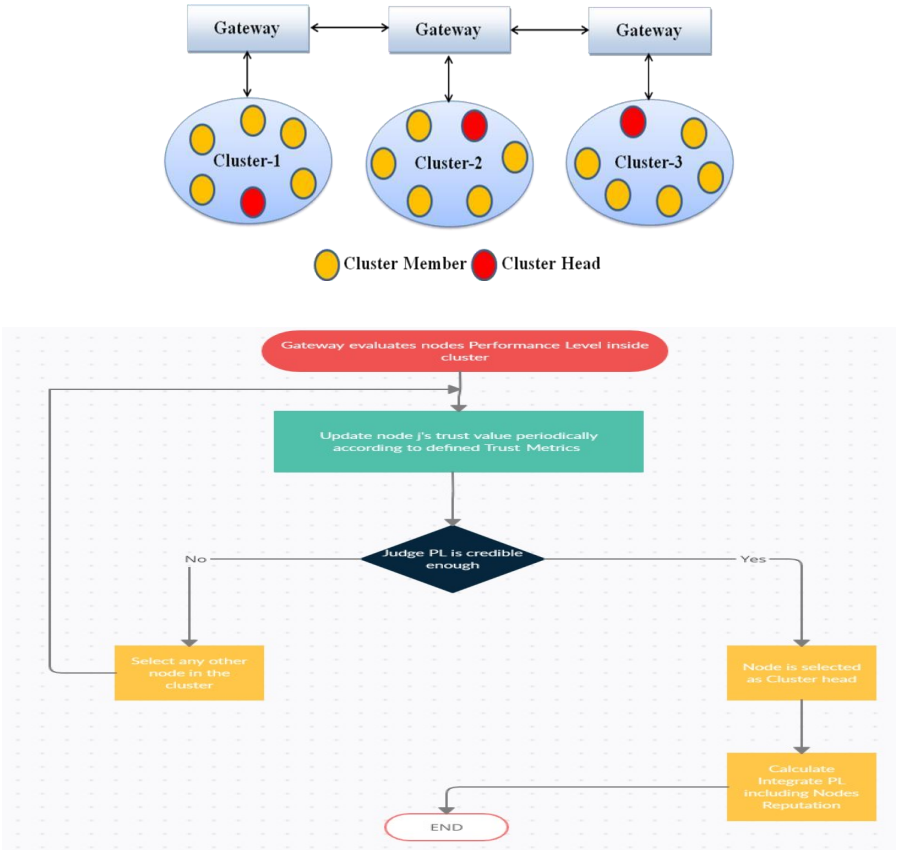

Fig.1.6 Multi-Cluster Communication through Gateway

Step-6: For intra cluster interactions, only Performance Level of Custer Head w.r.to service requester J is enough to decide if resource allocation will be granted or not, reputation component is not required in this case, since CH will provide feedback of node in the direct interaction component of trust metrics. In case of inter cluster interactions; integrated trust value is required which will keep both Performance Levels of Custer Head w.r.to service requester and reputation score of the service requester (Fig.1.4).

Result: With this methodology not just, saves the number of additional communications between the provider and requester, but also improves the network lifetime by saving energy consumption. All the transactions, service provider, and service requester are consistently under the supervision of respective CHs and edge nodes (Fig.1.5).

Different color notations are given to highlight the cluster head (CH) and cluster member (CM) in the cluster and follow a bidirectional communication channel with gateway nodes at all times. Every cluster will map to its nearest gateway node and further, the processed data will be sent to the sink node which can save the energy of clusters for prolonging network operations.

The complete trust management flow for our mechanism is highlighted through the flow diagram (Fig.1.6). After cluster formation, the gateway nodes will supervise the trust evaluation process. For every cluster, the same gateway or different gateway nodes will leverage trust metrics calculation based on trust properties. Trust performance level will determine the selection of the node as head and integrated PL will facilitate the provisioning of services to trustee or requester.[46] The gateway plays a significant part in dealing with the Cluster, further inter cluster correspondence of nodes. There are many famous platforms utilized in everyday life which can act as gateway associated with sensor, actuators or transducers (Table 1.1). Below gateways are following different architecture models, communication protocols, protocol stacks, and infrastructure usage and design of different IoT levels for operations. In real time applications, our approach needs to find out the suitable gateway nodes which can support our proposed trust management mechanism execution successfully. Also, we can identify special features and characteristics of every gateway along with its hardware details and the microcontroller embed these gateway nodes and connected to IoT devices[47]

Table 1 Basic IoT Platform and their Link Layer Protocols

Platform	Ethernet	Wi-Fi	Bluetooth
Arduino Yun	IEEE 802.310/100Mb/s	IEEE 802.11/b/g/n	No
STM32F4 discovery	IEEE 802.3, 10/100Mb/s	No	No
mBed	IEEE 802.3- 10/100Mb/s	No	No
Intel Edison	IEEE 802.3 10/100Mb/s	IEEE 802.11 a/b/g/n	Bluetooth 4.0, LE
WaRP7	No	802.11b/g/n	Bluetooth 4.1, Classic and low energy (LE).
SensorTile	No	No	Bluetooth 4.1, BLE
Raspberry Pi 3-Model B	IEEE 802.3 10/100Mb/s	IEEE 802.11/b/g/n	Bluetooth 4.1,Classic and LE
Beagle bone black	IEEE 802.3 10/100Mb/s	No	No
Samsung Artik 10	No	IEEE 802.11/b/g/n	Bluetooth 4.1 LE
Qualcomm DragonBoard 410c	No	802.11n 802.11a/b/g	Bluetooth 4.1, BLE

9. Result and Discussion

Our presented scheme is executed in the simulation environment considering different parameters as cited in Table 1. The simulation network consists of 100 nodes with a radio range of 100m following the 802.11b communication protocol. The experiment is carried out for 100sec and each node following PL routing finding a trustworthy node to send packets of 128 bytes size, the traffic source is of type sense application, which means devices will send packets after accumulating data and remain idle for sometime before data sense again. Our protocol follows the proposed algorithm for cluster formation, so 10 clusters are formed from 100 devices present in the network. The bandwidth of the network is 50 kbps with the IPV4 network protocol [48], [49].

Simulation results are obtained by comparing our cluster based distributed management scheme with the other cluster based schemes to measure trust level. The experiments are based on the analysis of trust level results with time and also communication interactions overhead with time. The honest nodes follow the implementation of our trust management protocol, while the dishonest nodes act maliciously by providing fake recommendations through good-mouthing, bad-mouthing, and self-promoting attacks to disrupt network communication. The initial recommendation for the trust value of all devices is set to 0.5.

TABLE 1.2. Simulation Parameters

Parameter	Value
No. of Nodes	100
Area Size	120x120m2
Number of Clusters	10
Mac	802.11b
Coverage	100m
Simulation Time	100s
Traffic Source	Sensing On/Off
Packet Size	128bytes
Routing Protocol	PL Routing Protocol
Malicious Nodes	10%
InitialQuality Recommendation	0.5
Bandwidth	50kbps
Network Protocol	IPV4
Initial Energy	100

In Fig.1.7 Our methodology doesn't permit the communication interaction overload to occur, which in turn consumes more energy and drains out the battery power very fast. Our protocol ensures secure communication inside and outside the cluster of nodes through CH and gateway nodes, so there is very little probability that malicious nodes will make any impact on device communications. Trust assessment and evaluation procedures of our trust solution diminish the influence of malicious nodes' attacks. Reduced communication interaction overload is a positive sign for the design of holistic trust management protocol, that improved network lifetime and saves more energy for devices.

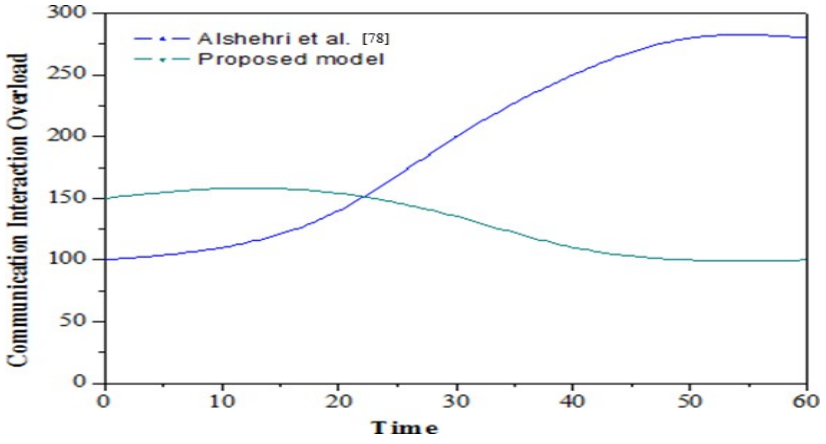

Fig. 1.7 Graph for Communication Interaction Overload

Fig.1.8 presents the observations of trust level with time. As it's noticed that trust level increases with time because malicious nodes are restricted to interfere in network communication. But, in other models trust value dips down further with time. IoT applications are most critical working in an uncertain environment holding sensitive data, definitely before sharing data node should be trustworthy to assign and reprocess further. Our trust mechanism is well suitable for providing security solution to IoT preventing security attacks. Cluster head (CH) and gateway nodes are authorized for intra-cluster and inter-cluster interactions with the help of trust value generated from the trust metrics, together both sensor and edge computing layers are addressing the security challenges with the limited capacity of nodes [50]. This model is very well implemented for resource constrained devices that are performing the critical task of providing data through REST API services. Also, other trust performance metrics can be evaluated in this cluster-based approach by varying the percentage of the malicious node in the network.

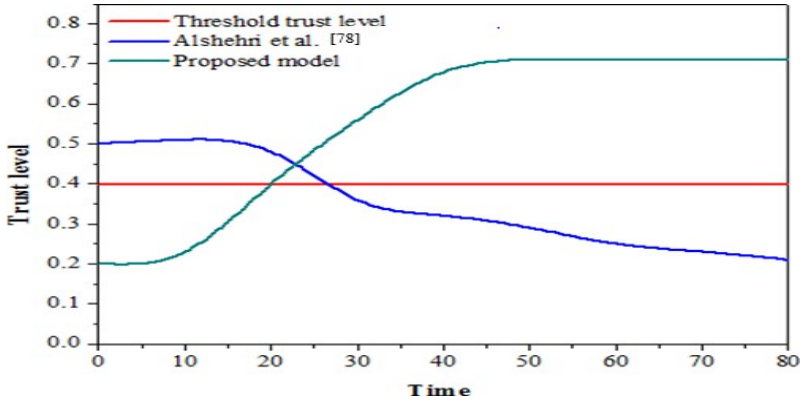

Fig.1.8. Graph for Trust Level

10. Summary

Security is a crucial part of heterogeneous devices' interactions and communications in IoT, therefore to provide the security holistic trust management mechanism is essential at this point. Our cluster priority based trust mechanism provides the necessary trust and ensures secure communication between the service provider and requester. The main advantages of our approach are the increase of trust level with time and also maximum trust level is achieved through minimum communication overhead. This solution is capable to curb the damage caused to the network is minimal by malicious nodes assaulting with bad mouthing attack, good mouthing attack, selective forwarding attacks as compared to other prototypes of trust mechanism. Also, gateway nodes of the edge computing layer help in data storage and processing facilitates inter-cluster communication of CHs, after then alleviates the burden on cluster nodes.
Simulation results show that improvement of network lifetime with efficient consumption of energy. Further, our future research is underway after finding malicious nodes inside the clusters, then what actions cluster head will take, will it consider the concept of node migration from one cluster to another. Migration of low trust/malicious nodes to other clusters will lead to creating high trust cluster zones before device interactions.

References

[1] Adithya. Potu, R.Jayalakshmi, Dr.K.Umpathy,2016,"Smart Paper Technology a Review Based On Concepts of E-Paper Technology",42-46.
[2] Aditya Gupta,Sudhir Mishra,Neeraj Bokde and Kishore Kulat,2016,"Need of Smart Water Systems In India",2216-2223.
[3] A. Menon, R. Sinha, D. Ediga, Prof. Subba Iyer 2013 "Implementation of Internet of Things in bus transport system of Singapore",08-17.
[4] Anshu Adwani, Kirti H. Madan, Rohit Hande,2015,"Smart Highways Systems for Future Cities",7292-7298.
[5] Ankita Gill, Amita Arora, Manvi Siwch,2017,"A Review On Applications Of Internet Of Things",17-21.
[6] Ankita More, Prof. Vivekanandreddy,2017,"E - Monitoring of Physical Health Care System using IoT",438-439.
[7] Arushi Singh, Divya Pathak, Prachi Pandit, Shruti Patil, Prof. Priti . C. Golar,2017,"IOT based Air and Sound Pollution Monitoring System",1273-1278.
[8] Ashwini Deshpande, Prajakta Pitale, Sangita Sanap, 2016 " Industrial Automation using Internet of Things (IOT)" ,1-4.
[9] Arko Djajadi, Michael Wijanarko,2016, "Ambient Environmental Quality Monitoring Using IoTSensor Network", 41-47.
[10] Anureet Kaur,2016 "Internet Of Things (Iot):Security And Privacy Concerns"161- 165.
[11] Chang-Su Ryu,2015, "IoT-based Intelligent for Fire Emergency Response Systems"161-168.
[12] Bharath Kumar Perumalla, M. Sunil Babu,2016,"An Intelligent Traffic and Vehicle Monitoring System using Internet of Things Architecture",853-856.
[13] B.Sobhan Babu,K. Srikanth,T.Ramanjaneyulu,I.Lakshmi Narayana,2016, "IoT for Healthcare",322-326.
[14] Bulipe Srinivas Rao, Prof. Dr. K. Srinivasa Rao, Mr. N. Ome,2016,"Internet of Things (IOT) Based Weather Monitoring system",312-319.
[15] Chen Qiang, Guang-ri Quan, Bai Yu and Liu Yang, 2013 " Research on Security Issues of the Internet of Things" ,1-10. ` 2
[16] Chandra Sukanya Nandyala and Haeng-Kon Kim,2016"From Cloud to Fog and IoT-Based Real-Time U-Healthcare Monitoring for Smart Homes and Hospitals",187- 196.
[17] Daiwat A. Vyas, Dvijesh Bhatt, Dhaval Jha,2016,"IoT: Trends, Challenges and Future Scope",186-199.
[18] Deshpande P. L. and Deshpande L.M., 2017 " Industrial Environmental Parameters Monitoring and Controlling Using IoT", 7-12.
[19] Divya Joshi Chanchal Kumari Abhishek Srivastava,2016, "Challenges And Data Mining Model For IoT",36-41.

[20] Dr.K Pratheep Moses, Dr.M.Elango,2017,"A critical Analysis of Smart Cities Approaches in India",1381-1383.
[21] Dr. A. Sumithra,J.Jane Ida,K. Karthika ,Dr. S. Gavaskar,2016,"A Smart Environmental Monitoring System Using Internet Of Things",261-265.
[22] Dhanashri Ajay konnur Dr. L K Ragha,2016, "Review Paper on Smart Sensor Network for Air Quality Monitoring"31-35.
[23] Deepak Kumar Rath,2016,"Arduino Based: Smart Light Control System",784-790.
[24] Farah Hussein Mohammed, Dr. Roslan Esmail, 2015 " Survey on IoT Services: Classifications and Applications", 2125-2128.
[25] Gurdip Singh Sodi,2016,"Internet Of Things- Integration And Semantic Interoperability Of Sensor Data Of Things In Heterogeneous Environments",174-178.
[26] Garvit Gupta, Shripal singh, Rajesh Saini, Shekhar Mahich, Ritesh Singh,2017,"IoT (Internet of things) Base Pollution Measurement system",561-563.
[27] G.Mamatha,2016,"Overview and Concept for IOT Models",20238-20241.
[28] Harshini Vijetha H, Dr. Nataraj K R,2017,"IOT Based Intelligent Traffic Control System",707-711.
[29] Haesung Lee, Kwangyoung Kim and Joonhee Kwon,2016,"A Pervasive Interconnection Technique for Efficient Information Sharing in Social IoT Environment",9-22.
[30] Jihwa Lee, Jong Wook Kim, Il-Min Kim, Sae-Hong Cho,2015 "Study for the Effectiveness of IoT Technologies Applied Advertisement",22-25.
[31] Govinda K. Saravanaguru R.A.K,2016, "Review on IOT Technologies",2848 2853.
[32] J. Ann Roseela, Dr. S. Ravi, Dr. M. Anand,2016, "RF Based Node Location and Mobility Tracking in IoT",5714-5718. ` 3
[33] Jiehan Zhou, Teemu Leppänen, Erkki Harjula,2013,"CloudThings: a Common Architecture for Integrating the Internet of Things with Cloud Computing",651-657.
[34] J. Sathish Kumar,Dhiren R. Patel,2014,"A Survey on Internet of Things: Security and Privacy Issues",20-27.
[35] J.Sherly,D.Somasundareswari,2015,"Internet Of Things Based Smart Transportation Systems",1207-1210.
[36] K.Yogitha, V.Alamelumangai,2016, "Recent Trends And Issues In Iot",50-56
[37] Karandeep Kaur,2016,"A study of the role of Cloud services in the implementation of Internet of Things (IoT)",545-548.
[38] KalyaniGhute,GayatriThakare,MayuriWahane,AkshayHoley,Prof.Mayuri.M.Soni,2 017,"IOT Based Smart Garbage Monitoring And Air Pollution Control System",6013- 6016.
[39] Keyur K Patel, Sunil M Patel,2016,"Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges",6122-6131.
[40] Karan A. Shah, Ms. Jasmine Jha, Manmitsinh Zala, Nirav Khetra,2015,"Improvement of Traffic Monitoring System by Density and Flow Control for Indian Road System using IoT",167-170.
[41] K.N.V. Satyanarayana, S.R.N. Reddy, P.V.Y.N Sai Teja, MD. Basit Habibuddin,2016 " IOT Based Smart Weather Station Using Raspberry-PI3",1-6.
[42] K.N.V.Satyanarayana,S.R.N. Reddy, K.N.V.Suresh Varma & P. Kanaka Raju,2017,"Mobile App & IoT Based Smart Weather Station",1-8.
[43] L.Deepika, B. Divya, P. Jeevitha, P. Ramkumar, T. Boobalan ,2016 "IoT Based Prepaid Electricity",611-613.
[44] Mane S.P, Kavathekar G.S, Jadhav S.T,2014,"A Zigbee Based Smart Sensing Platform forEnvironmental Monitoring",735-738.
[45] Meetali V. Rasal, Prof. Jaideep G. Rana,2016,"Raspberry Pi Based Weather Monitoring System",119-122.
[46] Ms. Yogita Pundir, Ms. Nancy Sharma, Dr. Yaduvir Singh,2016,"Internet of Things (IoT) : Challenges and Future Directions",960-964.
[47] Meenakshi Nadimpalli,2017,"Internet of Things – Future Outlook",1-5.
[48] Megh Patel, Abhilash Singh Meena,2017,"The Future of Internet of Things",30 307.
[49] Mimi Cherian,2017,"Study of Internet of Things using Simulator",7-16. ` 4
[50] Ms. Supriya Chandrakant Padwal, Mr. Suraj Vishnu Kurde,2016,"Long-Term Environment Monitoring for IOT Applications using Wireless Sensor Network",50-55.